Index to Volume 13

BOYAR, J.: Short Non-Interactive Cryptographic Proofs 449
CANETTI, R.: Maintaining Authenticated Communication in the Presence of Break-Ins 61
CANETTI, R.: Randomness versus Fault-Tolerance 107
CANETTI, R.: Security and Composition of Multiparty Cryptographic Protocols 143
COPPERSMITH, D.: On Polynomial Approximation of the Discrete Logarithm and the Diffie–Hellman Mapping 339
DAMGÅRD, I.: *see* BOYAR, J. 449
DAWSON, E.: *see* GOLIĆ, J. DJ. 245
FISCHLIN, R.: Stronger Security Proofs for RSA and Rabin Bits 221
FRANKLIN, M.: Secure Communication in Minimal Connectivity Models 9
GENNARO, R.: Robust and Efficient Sharing of RSA Functions 273
GENNARO, R.: RSA-Based Undeniable Signatures 397
GISIN, N.: *see* ZBINDEN, H. 207
GOLDREICH, O.: Preface 1
GOLIĆ, J. DJ.: Fast Correlation Attacks on the Summation Generator 245
HALEVI, S.: *see* CANETTI, R. 61
HERZBERG, A.: *see* CANETTI, R. 61
HIRT, M.: Player Simulation and General Adversary Structures in Perfect Multiparty Computation 31
HUTTNER, B.: *see* ZBINDEN, H. 207
JACOBSON, M. J., JR.: Computing Discrete Logarithms in Quadratic Orders .. 473
JARECKI, S.: *see* GENNARO, R. 273
KNUDSEN, L. R.: A Detailed Analysis of SAFER K 417
KRAWCZYK, H.: *see* GENNARO, R. 273, 397
KUSHILEVITZ, E.: *see* CANETTI, R. 107
MAURER, U.: *see* HIRT, M. 31
MULLER, A.: *see* ZBINDEN, H. 207
OSTROVSKY, R.: *see* CANETTI, R. 107
PAULUS, S.: A New Public-Key Cryptosystem over a Quadratic Order with Quadratic Decryption Time 263
PERALTA, R.: *see* BOYAR, J. 449
PETRANK, E.: CBC MAC for Real-Time Data Sources 315
POINTCHEVAL, D.: Security Arguments for Digital Signatures and Blind Signatures 361
POLLARD, J. M.: Kangaroos, Monopoly and Discrete Logarithms 437
RABIN, T.: *see* GENNARO, R. 273, 397
RACKOFF, C.: *see* PETRANK, E. 315
ROSÉN, A.: *see* CANETTI, R. 107
SALMASIZADEH, M.: *see* GOLIĆ, J. DJ. 245
SCHNORR, C. P.: *see* FISCHLIN, R. 221

SHPARLINSKI, I.: *see* COPPERSMITH, D. 339
STERN, J.: *see* POINTCHEVAL, D. 361
TAKAGI, T.: *see* PAULUS, S. 263
TITTEL, W.: *see* ZBINDEN, H. 207
WRIGHT, R. N.: *see* FRANKLIN, M. 9
ZBINDEN, H.: Practical Aspects of Quantum Cryptographic Key Distribution 207
ZHANG, M.: Maximum Correlation Analysis of Nonlinear Combining Functions in Stream Ciphers 301